

UNITED STATES PATENT APPLICATION

FOR

METHOD AND SYSTEM FOR MAINTAINING SECURE ACCESS TO WEB SERVER  
SERVICES USING SERVER-DELEGATED PERMISSIONS

BY

CARL A. GUNTER, ROBERT LEVAS AND MICHAEL C. BERRY

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
989  
990  
991  
992  
993  
994  
995  
996  
997  
998  
999  
1000  
1001  
1002  
1003  
1004  
1005  
1006  
1007  
1008  
1009  
1010  
1011  
1012  
1013  
1014  
1015  
1016  
1017  
1018  
1019  
1020  
1021  
1022  
1023  
1024  
1025  
1026  
1027  
1028  
1029  
1030  
1031  
1032  
1033  
1034  
1035  
1036  
1037  
1038  
1039  
1040  
1041  
1042  
1043  
1044  
1045  
1046  
1047  
1048  
1049  
1050  
1051  
1052  
1053  
1054  
1055  
1056  
1057  
1058  
1059  
1060  
1061  
1062  
1063  
1064  
1065  
1066  
1067  
1068  
1069  
1070  
1071  
1072  
1073  
1074  
1075  
1076  
1077  
1078  
1079  
1080  
1081  
1082  
1083  
1084  
1085  
1086  
1087  
1088  
1089  
1090  
1091  
1092  
1093  
1094  
1095  
1096  
1097  
1098  
1099  
1100  
1101  
1102  
1103  
1104  
1105  
1106  
1107  
1108  
1109  
1110  
1111  
1112  
1113  
1114  
1115  
1116  
1117  
1118  
1119  
1120  
1121  
1122  
1123  
1124  
1125  
1126  
1127  
1128  
1129  
1130  
1131  
1132  
1133  
1134  
1135  
1136  
1137  
1138  
1139  
1140  
1141  
1142  
1143  
1144  
1145  
1146  
1147  
1148  
1149  
1150  
1151  
1152  
1153  
1154  
1155  
1156  
1157  
1158  
1159  
1160  
1161  
1162  
1163  
1164  
1165  
1166  
1167  
1168  
1169  
1170  
1171  
1172  
1173  
1174  
1175  
1176  
1177  
1178  
1179  
1180  
1181  
1182  
1183  
1184  
1185  
1186  
1187  
1188  
1189  
1190  
1191  
1192  
1193  
1194  
1195  
1196  
1197  
1198  
1199  
1200  
1201  
1202  
1203  
1204  
1205  
1206  
1207  
1208  
1209  
1210  
1211  
1212  
1213  
1214  
1215  
1216  
1217  
1218  
1219  
1220  
1221  
1222  
1223  
1224  
1225  
1226  
1227  
1228  
1229  
1230  
1231  
1232  
1233  
1234  
1235  
1236  
1237  
1238  
1239  
1240  
1241  
1242  
1243  
1244  
1245  
1246  
1247  
1248  
1249  
1250  
1251  
1252  
1253  
1254  
1255  
1256  
1257  
1258  
1259  
1260  
1261  
1262  
1263  
1264  
1265  
1266  
1267  
1268  
1269  
1270  
1271  
1272  
1273  
1274  
1275  
1276  
1277  
1278  
1279  
1280  
1281  
1282  
1283  
1284  
1285  
1286  
1287  
1288  
1289  
1290  
1291  
1292  
1293  
1294  
1295  
1296  
1297  
1298  
1299  
1300  
1301  
1302  
1303  
1304  
1305  
1306  
1307  
1308  
1309  
1310  
1311  
1312  
1313  
1314  
1315  
1316  
1317  
1318  
1319  
1320  
1321  
1322  
1323  
1324  
1325  
1326  
1327  
1328  
1329  
1330  
1331  
1332  
1333  
1334  
1335  
1336  
1337  
1338  
1339  
1340  
1341  
1342  
1343  
1344  
1345  
1346  
1347  
1348  
1349  
1350  
1351  
1352  
1353  
1354  
1355  
1356  
1357  
1358  
1359  
1360  
1361  
1362  
1363  
1364  
1365  
1366  
1367  
1368  
1369  
1370  
1371  
1372  
1373  
1374  
1375  
1376  
1377  
1378  
1379  
1380  
1381  
1382  
1383  
1384  
1385  
1386  
1387  
1388  
1389  
1390  
1391  
1392  
1393  
1394  
1395  
1396  
1397  
1398  
1399  
1400  
1401  
1402  
1403  
1404  
1405  
1406  
1407  
1408  
1409  
1410  
1411  
1412  
1413  
1414  
1415  
1416  
1417  
1418  
1419  
1420  
1421  
1422  
1423  
1424  
1425  
1426  
1427  
1428  
1429  
1430  
1431  
1432  
1433  
1434  
1435  
1436  
1437  
1438  
1439  
1440  
1441  
1442  
1443  
1444  
1445  
1446  
1447  
1448  
1449  
1450  
1451  
1452  
1453  
1454  
1455  
1456  
1457  
1458  
1459  
1460  
1461  
1462  
1463  
1464  
1465  
1466  
1467  
1468  
1469  
1470  
1471  
1472  
1473  
1474  
1475  
1476  
1477  
1478  
1479  
1480  
1481  
1482  
1483  
1484  
1485  
1486  
1487  
1488  
1489  
1490  
1491  
1492  
1493  
1494  
1495  
1496  
1497  
1498  
1499  
1500  
1501  
1502  
1503  
1504  
1505  
1506  
1507  
1508  
1509  
1510  
1511  
1512  
1513  
1514  
1515  
1516  
1517  
1518  
1519  
1520  
1521  
1522  
1523  
1524  
1525  
1526  
1527  
1528  
1529  
1530  
1531  
1532  
1533  
1534  
1535  
1536  
1537  
1538  
1539  
1540  
1541  
1542  
1543  
1544  
1545  
1546  
1547  
1548  
1549  
1550  
1551  
1552  
1553  
1554  
1555  
1556  
1557  
1558  
1559  
1560  
1561  
1562  
1563  
1564  
1565  
1566  
1567  
1568  
1569  
1570  
1571  
1572  
1573  
1574  
1575  
1576  
1577  
1578  
1579  
1580  
1581  
1582  
1583  
1584  
1585  
1586  
1587  
1588  
1589  
1590  
1591  
1592  
1593  
1594  
1595  
1596  
1597  
1598  
1599  
1600  
1601  
1602  
1603  
1604  
1605  
1606  
1607  
1608  
1609  
1610  
1611  
1612  
1613  
1614  
1615  
1616  
1617  
1618  
1619  
1620  
1621  
1622  
1623  
1624  
1625  
1626  
1627  
1628  
1629  
1630  
1631  
1632  
1633  
1634  
1635  
1636  
1637  
1638  
1639  
1640  
1641  
1642  
1643  
1644  
1645  
1646  
1647  
1648  
1649  
1650  
1651  
1652  
1653  
1654  
1655  
1656  
1657  
1658  
1659  
1660  
1661  
1662  
1663  
1664  
1665  
1666  
1667  
1668  
1669  
1670  
1671  
1672  
1673  
1674  
1675  
1676  
1677  
1678  
1679  
1680  
1681  
1682  
1683  
1684  
1685  
1686  
1687  
1688  
1689  
1690  
1691  
1692  
1693  
1694  
1695  
1696  
1697  
1698  
1699  
1700  
1701  
1702  
1703  
1704  
1705  
1706  
1707  
1708  
1709  
1710  
1711  
1712  
1713  
1714  
1715  
1716  
1717  
1718  
1719  
1720  
1721  
1722  
1723  
1724  
1725  
1726  
1727  
1728  
1729  
1730  
1731  
1732  
1733  
1734  
1735  
1736  
1737  
1738  
1739  
1740  
1741  
1742  
1743  
1744  
1745  
1746  
1747  
1748  
1749  
1750  
1751  
1752  
1753  
1754  
1755  
1756  
1757  
1758  
1759  
1760  
1761  
1762  
1763  
1764  
1765  
1766  
1767  
1768  
1769  
1770  
1771  
1772  
1773  
1774  
1775  
1776  
1777  
1778  
1779  
1780  
1781  
1782  
1783  
1784  
1785  
1786  
1787  
1788  
1789  
1790  
1791  
1792  
1793  
1794  
1795  
1796  
1797  
1798  
1799  
1800  
1801  
1802  
1803  
1804  
1805  
1806  
1807  
1808  
1809  
1810  
1811  
1812  
1813  
1814  
1815  
1816  
1817  
1818  
1819  
1820  
1821  
1822  
1823  
1824  
1825  
1826  
1827  
1828  
1829  
1830  
1831  
1832  
1833  
1834  
1835  
1836  
1837  
1838  
1839  
1840  
1841  
1842  
1843  
1844  
1845  
1846  
1847  
1848  
1849  
1850  
1851  
1852  
1853  
1854  
1855  
1856  
1857  
1858  
1859  
1860  
1861  
1862  
1863  
1864  
1865  
1866  
1867  
1868  
1869  
1870  
1871  
1872  
1873  
1874  
1875  
1876  
1877  
1878  
1879  
1880  
1881  
1882  
1883  
1884  
1885  
1886  
1887  
1888  
1889  
1890  
1891  
1892  
1893  
1894  
1895  
1896  
1897  
1898  
1899  
1900  
1901  
1902  
1903  
1904  
1905  
1906  
1907  
1908  
1909  
1910  
1911  
1912  
1913  
1914  
1915  
1916  
1917  
1918  
1919  
1920  
1921  
1922  
1923  
1924  
1925  
1926  
1927  
1928  
1929  
1930  
1931  
1932  
1933  
1934  
1935  
1936  
1937  
1938  
1939  
1940  
1941  
1942  
1943  
1944  
1945  
1946  
1947  
1948  
1949  
1950  
1951  
1952  
1953  
1954  
1955  
1956  
1957  
1958  
1959  
1960  
1961  
1962  
1963  
1964  
1965  
1966  
1967  
1968  
1969  
1970  
1971  
1972  
1973  
1974  
1975  
1976  
1977  
1978  
1979  
1980  
1981  
1982  
1983  
1984  
1985  
1986  
1987  
1988  
1989  
1990  
1991  
1992  
1993  
1994  
1995  
1996  
1997  
1998  
1999  
2000  
2001  
2002  
2003  
2004  
2005  
2006  
2007  
2008  
2009  
2010  
2011  
2012  
2013  
2014  
2015  
2016  
2017  
2018  
2019  
2020  
2021  
2022  
2023  
2024  
2025  
2026  
2027  
2028  
2029  
2030  
2031  
2032  
2033  
2034  
2035  
2036  
2037  
2038  
2039  
2040  
2041  
2042  
2043  
2044  
2045  
2046  
2047  
2048  
2049  
2050  
2051  
2052  
2053  
2054  
2055  
2056  
2057  
2058  
2059  
2060  
2061  
2062  
2063  
2064  
2065  
2066  
2067  
2068  
2069  
2070  
2071  
2072  
2073  
2074  
2075  
2076  
2077  
2078  
2079  
2080  
2081  
2082  
2083  
2084  
2085  
2086  
2087  
2088  
2089  
2090  
2091  
2092  
2093  
2094  
2095  
2096  
2097  
2098  
2099  
2100  
2101  
2102  
2103  
2104  
2105  
2106  
2107  
2108  
2109  
2110  
2111  
2112  
2113  
2114  
2115  
2116  
2117  
2118  
2119  
2120  
2121  
2122  
2123  
2124  
2125  
2126  
2127  
2128  
2129  
2130  
2131  
2132  
2133  
2134  
2135  
2136  
2137  
2138  
2139  
2140  
2141  
2142  
2143  
2144  
2145  
2146  
2147  
2148  
2149  
2150  
2151  
2152  
2153  
2154  
2155  
2156  
2157  
2158  
2159  
2160  
2161  
2162  
2163  
2164  
2165  
2166  
2167  
2168  
2169  
2170  
2171  
2172  
2173  
2174  
2175  
2176  
2177  
2178  
2179  
2180  
2181  
2182  
2183  
2184  
2185  
2186  
2187  
2188  
2189  
2190  
2191  
2192  
2193  
2194  
2195  
2196  
2197  
2198  
2199

## CROSS REFERENCE TO RELATED APPLICATIONS

[0001] Not applicable.

## STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH

[0002] Not applicable.

## BACKGROUND OF THE INVENTION

### FIELD OF THE INVENTION

[0003] The present invention is directed generally to methods and systems for maintaining secure access to services maintained on web servers.

### DESCRIPTION OF THE BACKGROUND

[0004] Public key cryptographic systems offer a number of advantages over the use of shared secrets such as passwords. For example, private keys cannot be guessed, and public keys can be sent in cleartext over the Internet. Chains of public key certificates can be used to bind names to keys based on a hierarchical or web-like system of authority. This allows parties to use public keys very broadly. For example, public key certificates are widely used on the World Wide Web (WWW) to provide authority for the binding of domain names to keys as part of the SSL protocol. This enables clients to authenticate web servers in sensitive exchanges such as credit card purchases. The SSL protocol also allows for client public key authentication, permitting the client to supply a public key certificate and authenticate by showing knowledge of the appropriate private key.

[0005] While public key certificates that bind a name to a key are very advantageous, it is often desirable to offer another form of certificate, called an attribute certificate, that binds general properties to a key or name. For example, an attribute certificate may indicate that a public key belongs to an individual who is an employee of a company. This information can be included in a public key certificate, but doing so may introduce undesirable maintenance requirements for the public key certificate. For example, if an individual has a certificate binding his name to a key and also indicating that he is the employee of a company, then the certificate will need to be revoked if he leaves the company. If instead he had a public key certificate binding his name to a key and, in addition, an attribute certificate indicating that his key belonged to an individual working for the company in question, then only the attribute certificate would need to be revoked if he left the company. The situation is even clearer when the attribute certificate is intended for

a specific or short-lived purpose like a permission to access a resource for a limited time. If each such permission had to be included in the public key certificate then this certificate would need to be changed very frequently.

[0006] Formats and verification rules for attribute certificates have been described in a number of major standards. There are also sophisticated systems available for creating chains of certificates for access to a resource and verifying that a proper sequence of delegations leads from an authority entitled to grant and delegate a permission via a sequence of well-formed delegations to the party requesting the resource.

[0007] Despite numerous advantages of public key certificates and their use in connection with attribute certificates, their use by non-servers on the web is comparatively limited. To enable the use of attribute certificates on the web, a number of support functions are needed to create, distribute, and delegate permissions using typical web browsers, web servers, and Internet messaging systems.

#### BRIEF SUMMARY OF THE INVENTION

[0008] The current invention addresses the needs present in the prior art.

[0009] The present invention is directed to a method and system of providing secure access to a service on a service web server. A first permission is maintained at a permission web server. The first permission includes a label related to the service and a digital signature of a first user. A second user is provided access to the first permission upon the second user authenticating to the permission web server. The second user is provided a permission that includes the first permission and a permission link that includes the label and a digital signature of the permission web server. A request to access the service is received at the service web server from the second user, as well as the permission. The digital signature of the permission web server and the digital signature of the first user in the permission are verified. The second user is provided access to the service if the verification produces a positive result. Instead of, or in addition to, seeking access to the service himself, the second user may delegate permission to access the service to a subsequent user.

#### BRIEF DESCRIPTION OF THE DRAWINGS

[0010] The accompanying drawings, wherein like referenced numerals are employed to designate like parts or steps, are included to provide a further understanding of the invention, are

incorporated and constitute a part of this specification, and illustrate embodiments of the invention that together with the description serve to explain the principles of the invention.

[0011] In the drawings:

[0012] Figure 1A illustrates a message sequence chart of a preferred embodiment of the present invention.

[0013] Figure 1B illustrates a system of one embodiment of the present invention.

[0014] Figure 1C illustrates a message sequence chart of a preferred embodiment of the present invention.

[0015] Figure 1D illustrates exemplary data structures for two permissions.

[0016] Figure 1E provides an example of a web page that allows a user to configure a resource for a permission in accordance with the present invention.

[0017] Figure 1F provides an example of a web page that presents information that is the subject of a resource for a permission in accordance with the present invention.

[0018] Figure 2A illustrates a message sequence chart of a preferred embodiment of the present invention.

[0019] Figure 2B illustrates a system of one embodiment of the present invention.

[0020] Figure 3A illustrates a message sequence chart of a preferred embodiment of the present invention.

[0021] Figure 3B illustrates a system of one embodiment of the present invention.

[0022] Figure 3C illustrates exemplary data structures for a permission and two permission links.

[0023] Figure 4A illustrates a message sequence chart of a preferred embodiment of the present invention.

[0024] Figure 4B illustrates a system of one embodiment of the present invention.

[0025] Figure 4C illustrates an exemplary data structure for a multi-subject permission.

[0026] Figure 5 is a flow diagram illustrating a method of providing secure access to a service on a web server in accordance with a preferred embodiment of the present invention.

[0027] Figure 6 is a flow diagram illustrating a method of providing secure access to a service on a web server in accordance with a preferred embodiment of the present invention.

[0028] Figure 7 is a flow diagram illustrating a method of providing secure access to a service on a web server in accordance with a preferred embodiment of the present invention.

[0029] Figure 8 is a flow diagram illustrating a method of providing secure access to a service on a web server in accordance with a preferred embodiment of the present invention.

[0030] Figure 9 is a flow diagram illustrating a method of providing secure access to a service on a web server in accordance with a preferred embodiment of the present invention.

[0031] Figure 10 is a flow diagram illustrating a method of providing secure access to a service on a web server to each of a plurality of recipients of an electronic message in accordance with a preferred embodiment of the present invention.

#### DETAILED DESCRIPTION

[0032] Reference will now be made in detail to the preferred embodiments of the present invention, examples of which are illustrated in the accompanying drawings. It is to be understood that the figures and descriptions of the present invention included herein illustrate and describe elements that are of particular relevance to the present invention, while eliminating, for purposes of clarity, other elements. Those of ordinary skill in the art will recognize that other elements may be desirable and/or required in order to implement the present invention.

However, because such elements are well known in the art, and because they do not facilitate a better understanding of the present invention, a discussion of such elements is not provided herein.

[0033] The invention described herein relates to creation and manipulation of permissions, signed with a digital signature. There are a variety of different ways for creating such permissions. For example, permissions may have a form similar to ones defined in IETF RFC 2693, Simple Public Key Infrastructure Certificate Theory. The preferred embodiments disclosed herein describe permissions that are created through use of public/private key encryption techniques. However, other methods of creating a digital signature are known to those skilled in the art and may be used in connection with the present invention.

[0034] In one aspect of the invention, a user may delegate a permission to a server and may allow the server to delegate this permission to parties that are able to access it. This allows the first party to effectively delegate access to a resource to a collection of parties as determined by the permission server. This can be done even if the permission was granted to the first user via a chain of delegated permissions for a resource controlled by a third party. The resulting system enables authenticated users to “surf” through the system and automatically gain credentials that testify to their acquired right to access resources on other servers.

[0035] Figure 1A depicts a message sequence chart illustrating a preferred embodiment of a method of providing secure access to a service maintained on a server in accordance with the present invention. The term service referred to herein relates to accessing or delivery of content, referring broadly to any object, data, documents, files, directories, text, software, computer applications or other information. In step 112, a first user employs client issuer 104 to access permission server 106. Permission server 106 enables the first user to determine a label that relates to the service. For example, the label could comprise a query against a database that requests the desired information. The label may be a URL that identifies the location of the service on the web or may include such a URL. Alternatively, the label does not include a URL, but instead allows the URL indicating the location of the service to be determined from another source. In this case, the label represents a status from which benefits derive (i.e. the ability to access the service) rather than identifying the service particularly. The label may be associated with the URL using many different algorithms. By way of example, the label may include a URL within the domain of the URL that identifies the location of the desired service. In another example, the label may include a public key that is mentioned in the web site supporting the desired service.

[0036] A first permission link, including the label, is created at permission server 106 and, in step 114, provided to the first user at client issuer 104. In step 116, the first user requests from key server 102 the public key of a second user. In step 118, key server 102 provides the key to the first user at client issuer 104. The first user creates a second permission link, including the label, at client issuer 104. In step 120, the first user sends a permission (that includes the first permission link and the second permission link) to the second user at client subject 108. In step 122, the second user authenticates to application server 110 using his private key to identify himself and supplies the permission seeking authorization to access the service. Application server 110 verifies the information contained in the permission. In step 124, application server 110 provides the second user with access to the service based on an analysis of the information in the permission.

[0037] Figure 1B depicts a preferred embodiment of a system 100 for carrying out the methods described with reference to Figure 1A. A first user employs the web browser 128 on client issuer 104 (which may be a personal computer) to access permission server 106 via web server 132. Using server delegation module 136 on permission server 106, the first user determines a label

that relates to an application 146 on application server 110, as discussed with reference to Figure 1A.

[0038] A first permission link is created by server delegation module 136 at permission server 106. The first permission link includes a digital signature created by permission server 106 based on a public key of the first user and the label. The identity of the first user is verified using access control module 134. Permission server 106 then provides the first permission link to the first user at client issuer 104. The first user then employs client delegation module 126 of client issuer 104 to request from key server 102 (which maintains a registry of public keys) the public key of a second user. Key server 102 returns the key to client delegation module 126. Using client delegation module 126, the first user creates a second permission link that includes the label, the public key of the second user and a digital signature of the first user. Using messaging user agent 130 of client issuer 104, the first user sends a permission (which includes the first permission link and the second permission link) to the second user using messaging user agent 138 of client subject 108. The permission may be provided by the first user to the second user by employing a messaging system, such as electronic mail or instant messaging, or by using a personal area network.

[0039] The second user, using web browser 140 of client subject 108, authenticates to application server 110 through web server 144 using its private key and seeks authorization to access the service by supplying the permission. Access control module 142 of application server 110 verifies the digital signatures in the permission and confirms that the public key of the second user as provided in the second permission link corresponds to the private key of the second user. Access control module 142 also confirms that validity conditions included in the permission are met (such as whether the permission validity time period has expired). Upon verification, application server 110 allows the second user access to the application 146.

[0040] In some embodiments, the various components and functionality of permission server 106 and application server 110 may be located on one server, for example, server 1000 shown in Figure 1B. In other embodiments, the first and second users may be the same person (e.g., one person may want to delegate a permission from one client to another). For instance, a user may want to create and delegate to himself a permission that provides him with easy access to application 146 at a future time. For example, the user may want to create a permission for use while the user is on the road.

[0041] In an alternate preferred embodiment, in step 114 of Figure 1A, the permission server 106 does not create a permission for the first user and, instead, provides to the user only the label determined by the first user. With reference to Figure 1B, the first user employs client delegation module 126 of client issuer 104 to request from key server 102 the public key of a second user, and key server 102 provides the key to client delegation module 126 (steps 116 and 118 of Figure 1A). Using client delegation module 126, the first user creates a permission that includes the label, the public key of a second user and a digital signature of the first user. The first user then sends the permission to the second user (step 120 of Figure 1A). The second user, using web browser 140 of client subject 108, authenticates to application server 110 using web server 144 and supplies the permission (step 122 of Figure 1A). Access control module 142 of application server 110 verifies the digital signature in the permission. Application server 110 allows the second user access the application 146 (step 124 of Figure 1A) based on an analysis of the permission.

[0042] In these embodiments, application server 110 may verify that the first user has the right to delegate access to the application using, for example, access control module 142. For example, access control module 142 may maintain an access control list ("ACL") that would allow it to confirm this fact.

[0043] Still another preferred embodiment of a method of providing secure access to a service on a server allows for numerous chained delegations, as illustrated in the message sequence chart of Figure 1C. In this embodiment, steps 112, 114, 116, 118 and 120 are the same as those described with reference to Figure 1A. However, in this embodiment, the delegation described in step 120 is repeated one or more times. Thus, the second user may create a subsequent permission link using the first client subject 108. The second user then sends a permission (comprising the first permission link, the second permission link and the subsequent permission link) to a subsequent user at second client subject 148 in step 120.

[0044] The subsequent user may then create a second subsequent permission link and delegate a permission (comprising the first permission link, the second permission link, the subsequent permission link and the second subsequent permission link) using second client subject 148 to a second subsequent user at third client subject 150 in step 120. This series of delegations could continue any number of times. Then, in step 122, the Nth subsequent user employs the Nth client subject 152 and authenticates to application server 110 using the Nth permission.



Application server 110 verifies each digital signature in each permission link in the Nth permission and confirms that the public keys of each user as provided in each permission link corresponds to the private keys of such user. In step 124, application server 110 provides the Nth subsequent user access to the service.

[0045] As mentioned above, the service to which a user ultimately is provided access may not be one located at a particular URL determined by the first user. Instead, the service to which the second or subsequent user is provided access may be one derived from the URL. For example, the permission provided to the second or subsequent user may include the authority to access a particular domain. Authority to access other web pages within the domain are implied from authority to access the domain. In a particular example, the permission may include authority to access the home page of a particular web site. However, when the second or subsequent user exercises the authority delegated to him, such user is given access to an internal page of web site, rather than or in addition to the home page. Authority to access to the internal page is implied by the user's authority to access the home page. Thus, the resource to which the second user gained access was not specifically named by the URL determined by the user, but authorization to access to the resource was implied by authorization to access to the URL.

[0046] Figure 1D illustrates exemplary data structures of permissions that may be used in connection with the present invention. These permissions are constructed using public/private key encryption techniques. Permission link 160 of Figure 1D may be created by permission server 106 and returned to client issuer 104 in step 114 of Figure 1A. Permission link 160 includes the label 161 associated with the service (e.g., application 146 of Figure 1B), the public key 162 of client issuer 104, and the private key 164 of permission server 106. Permission link 160 may also include validity conditions 163, such as the validity time period for permission link 160 and whether the permission includes authority to further delegate the label. Each of these items is signed with digital signature 165 of the permission server 106, which cryptographically binds the identity of the permission server 106 to each of the items.

[0047] With reference to Figure 1A, upon obtaining the public key of the client subject 108 from key server 102, client issuer 104 may create permission link 170 (shown in Figure 1D). Permission link 170 includes label 171, the public key 172 of client subject 108, and the private key 174 of client issuer 104. Permission link 170 may also include validity conditions 173, such as the validity time period for permission link 170 and/or other information (e.g., whether the

permission included permission to further delegate). Each of these items is signed with digital signature 175 of client issuer 104, which cryptographically binds the identity of the client issuer to each of these items. Permission link 160 and permission link 170 are then chained to form a permission, which is, for example, delegated in step 120 of Figure 1A to client subject 108. In alternative embodiments of the present invention, the permissions links are nested rather than chained. In the case of nested permissions, the label would not be repeated, assuming it remains unchanged. Also, in the case of nested permissions, the signature must include some material from the previous links.

[0048] The permissions used in connection with the present invention may be validated in accordance with a number of techniques (depending primarily on the technique used to create the digital signature) that are known to those skilled in the art. One example of rules for verification is described in IETF RFC 2693 Simple Public Key Infrastructure Certificate Theory. In general, such validation typically includes verifying the signatures in each permission link (e.g., digital signature 165 and digital signature 175) as well as performing chain checking to ensure, for example, that the label included in each permission link represents the same or less authority presented in each of the preceding permissions.

[0049] An illustrative example of the methods and systems described with reference to Figures 1A and 1B is shown with reference to Figures 1E and 1F. In this example, a user wishes to provide information about the user's employment to a company from which the user seeks to obtain a mortgage. The user employs screen 190, shown in Figure 1E, to select the items to which he wishes to provide the mortgage company access. Here, the user determines that he wishes to provide the mortgage company his job title, salary and period of employment and indicates the same on screen 190. The user then clicks on the "create" button. In doing so, in this example, the user is creating a label that comprises a query against a database to be submitted ultimately by the mortgage company to learn the information. The label is included in a first permission link, as described previously herein. Upon creating the permission link, it is returned, for example, as an attachment in an e-mail to the user or provided within the user's browser (which can then be saved, opened or otherwise manipulated). The user may then create a second permission link and send it, along with the first permission link, to the mortgage company. This may be done, for example, by way of a messaging system such as electronic mail.

[0050] The mortgage company may then use the permission (which includes the first permission link and the second permission link) to attempt to gain access via the web to the information. Upon verifying the information in the permission, the mortgage company is presented with screen 192 of Figure 1F, which displays the information identified by the first user's query. In the preferred embodiment of the present invention, the information displayed on screen 192 is not merely a static list information but, instead, is representative of an ongoing service that obtains the information identified by the first user's query each time it is requested. Thus, the information displayed is dynamic and changes in accordance with any changes made in the database that stores the information. For example, if the user's job title or salary changes, and this change is reflected in the database against which the query is run, the change will be reflected in screen 192 upon the mortgage company accessing it. This feature may be particularly valuable in other contexts in which the same resource is accessed frequently and the information to be obtained from that resource is variable.

[0051] Figure 2A depicts a message sequence chart illustrating another preferred embodiment of a method of providing secure access to a service maintained on a web server in accordance with the present invention. In step 208, a first user employs the client issuer 202 to request from key server 201 the public key of the individual to whom the first user wishes to delegate permission to access the service. In step 210, the key is returned to client issuer 202. In step 212, the first user employs client issuer 202 to inform the second user, by sending an electronic message to client subject 206, that the second user must contact application server 204 to obtain access to the service. Upon the first user undertaking step 212, in step 214, client issuer 202 automatically updates application server 204 with the key information (e.g., the public key or information based on the public key) obtained in step 210 along with the label. In step 216, the second user, employing client subject 206, authenticates to application server 204 and, in step 218, application server 204 provides the second user access to the service.

[0052] Figure 2B depicts a preferred embodiment of a system 200 for carrying out the methods described with reference to Figure 2A. The first user employs client delegation module 208 of client issuer 202 to obtain from key server 201 the public key of the individual to whom the first user wishes to delegate permission to access the service. The first user then employs messaging user agent 210 of client issuer 202 to inform the second user at client subject 206, through messaging user agent 212, of the URL corresponding to the location of application server 204 so

that the second user may obtain access to the service (i.e., application 220). Upon the first user sending this message to the second user, messaging user agent 210 of client issuer 202 automatically contacts application server 204 through web server 218. Upon contacting application server 204, messaging user agent 210 updates access control module 216 with the key information of the second user obtained from key server 201 along with the label . The second user employs web browser 214 of client subject 206 to authenticate to application server 204 by providing its private key. Application server 204 confirms through access control module 216 that the private key of the second user corresponds to public key of the second user. If so, the second user is provided access to application 220.

**[0053]** The methods and systems described with reference to Figures 2A and 2B are useful in the same manner as those described with reference to Figures 1A and 1B. For example, an individual seeking a mortgage may wish to provide a mortgage company with information regarding the individual's employment in connection with the mortgage approval process. The first user may determine a URL corresponding to the desired information and send the mortgage company an electronic message (for example, an electronic mail message) that contains the URL. Upon the sending of the message, an ACL is updated with the public key information of the mortgage company. The mortgage company may then seek access to the information by supplying the URL and authenticating to the server using the mortgage company's private key.

**[0054]** Figure 3A is a message sequence chart that illustrates a method of providing secure access to a service located on a server in accordance with another preferred embodiment of the present invention. A first permission link is created, in one example, by the first user, and maintained on permission server 302. The first permission link provides permission server 302 with the authority to grant permission to access the service to individuals who are identified (e.g., by the first user), who request access to the service and who are properly authenticated and authorized. The individuals are identified and their public keys are stored in an ACL.

**[0055]** In step 308, a second user employs client subject 304 to authenticate to permission server 302, seeking permission to access the service. Assuming the second user is one identified by the first user to obtain permission to access the service, the second user obtains, in step 310, a second permission link created by permission server 302. In step 312, the second user employs client subject 304 to authenticate to application server 306 and supplies a permission (comprising the first permission link and the second permission link). In step 314, application server 306 verifies

the permission and, assuming a positive result, provides the second user with access to the service. In some embodiments, after step 310, the second user delegates the permission to a subsequent user (in addition to or in lieu of the second user performing step 312). The subsequent user may then, in step 312, authenticate to application server 306 using client subject 304 and supply his permission. The subsequent user's permission is verified in step 314 and, assuming a positive result, the subsequent user is provided access to the service.

[0056] A preferred embodiment of a system 300 that may be used to carry out the methods described with reference to Figure 3A is illustrated in Figure 3B. A first user creates and maintains in delegation chain store 326 of permission server 302 a permission link (for example, permission 340 of Figure 3C). In the preferred embodiment, the permission link includes a label relating to the service 332, a digital signature of the first user and a public key of permission server 302. The first user also stores in access control module 322 information regarding the identity (e.g., public key information) of the individual(s) to whom the permission may be delegated upon request.

[0057] A second user employs web browser 318 of client subject 304 to access permission server 302 through web server 320 and authenticates to permission server 302. Upon verifying with access control module 322 that the second user is one of the individuals to whom the permission may be delegated, server delegation application 324 delegates permission to access the service to the second user. Referring again to Figure 3C, the second user is delegated a permission that includes permission 340, described previously, and permission link 342. Permission link 342 includes, in one embodiment, the label 344, the public key 346 of the second user, validity conditions 348, the public key 350 of permission server 302, and is signed with the digital signature 352 of permission server 302.

[0058] Using web browser 318 of client subject 304, the second user contacts application server 306 through web server 330 and authenticates to application server 306 using the private key of the second user and supplies the permission. Using access control module 328, application server 306 verifies the information in the permission (i.e., the signatures, validity conditions, etc.). Upon successful verification, application server 306 provides the second user access to application 332.

[0059] As stated with reference to Figure 3A, the second user may also delegate a permission to access the service to a subsequent user. This delegation may be accomplished in a number of

different ways including email, PAN or the method described with reference to Figures 3A and 3B. The permission delegated to the subsequent user may be described with reference to Figure 3C. The subsequent permission includes permission 340, permission link 342 and subsequent permission link 360, (which includes the label 344, the public key 361 of the subsequent user, validity conditions 362, the public key 346 of the second user and digital signature 363 of the second user). Further delegations can be made by any subsequent user.

[0060] As with the systems and methods described in Figures 1A and 1B, the first and second user of the systems and methods described with reference to Figures 3A and 3B may be the same person. Similarly, the components of permission server 302 and application server 306 may be maintained on a single server 3000, shown in Figure 3B.

[0061] The methods and systems described with reference to Figures 3A and 3B are useful in many contexts. For example, the first user may know of many individuals who may potentially want permission from the first user to access a particular service. The first user is willing to grant such permissions, but does not know which of the many individuals will actually seek to access the service. The user may employ the methods and systems illustrated in Figures 3A and 3B to store a permission on permission server 302 to be delegated by permission server 302 only to particular individuals (within the larger class of individuals to whom the first user is willing to delegate permission) who request it.

[0062] The present invention also provides a method for distributing a permission to multiple recipients. Figure 4A is a message sequence chart that illustrates delegation of permission to multiple recipients using electronic messaging systems. In step 414, a first user employs client issuer 404 to contact key server 402 to request key information (i.e., the public keys) for the multiple individuals to whom the first user wants to delegate a permission. In step 416, the key information is returned. The client issuer 404 creates a single permission addressed to multiple recipients (including their keys) and sends it to message transfer system 406. Message transfer system 406 makes copies of the permission and sends a copy to each address. In this example, message transfer system 406 sends the permission to first client subject 408. Message transfer system 406 also sends the permission to second client subject 410. In other examples involving more than two recipients, the permission may be sent to more than two client subjects within the scope of the present invention. Second client subject 410 authenticates to application server 412 in step 424 by presenting its private key and seeks to gain authorization by supplying the

permission. First client subject 408 authenticates to application server 412 in step 426 by presenting its private key and seeks to gain authorization by supplying the permission. Upon successful authentication and authorization by the second client subject 410, in step 428, second client subject 410 obtains access to the service. In step 430, upon successful authentication and authorization of the first client subject 408, the first client subject 408 obtains access to the service.

[0063] Figure 4B illustrates a preferred embodiment of a system for carrying out the methods described with reference to Figure 4A. Using client delegation module 432, client issuer 404 contacts key server 402 to obtain the public key of each individual to whom the first user wants to delegate permission to access application 452. Client issuer 404 then creates a multi-subject permission using client delegation module 432.

[0064] This multi-subject permission is described with reference to Figure 4C, by way of example. The label 471 is included in permission 470, as is the public key of the first subject 472, the public key of the second subject 473, any validity conditions 474, and the public key of the issuer 475. Additional public keys may be included if the permission chain is intended for more than two subjects. Permission 470 is signed with the digital signature of the issuer 476, as illustrated in Figure 1D. Thus, the identities of the individuals that are to receive the electronic message, including their private keys, are automatically included in the permission and signed by the first user.

[0065] Returning again to Figure 4B, the permission (such as permission 470 of Figure 4C) provides that each of the individuals whose key information is included in the multi-subject permission should be provided access to application 452. Using messaging user agent 436 of client issuer 404, the first user sends the multi-subject permission in a single electronic mail message, addressed to each of the recipients, using message transfer system 406. Message transfer system 406 makes a copy of the multi-subject permission and sends it to each user that is to receive the permission (i.e., client subject 408 and client subject 410 through messaging user agent 438 and messaging user agent 442, respectively, in this example).

[0066] After receiving the permission from message transfer system 406, using web browser 446, second client subject 410 authenticates to application server 412 through web server 450. Using web browser 440, first client subject 408 authenticates to application server 412 through web server 450. Access control module 448 of application server 412 verifies the information in

the permission provided by the first client subject 408 and, upon verification, provides access to application 452. Similarly, but separately, access control module 448 of application server 412 verifies the information in the permission provided by the second client subject 410 and, upon verification, provides access to application 452.

[0067] As discussed elsewhere herein, the label included in the permission may either be a URL or may include a URL. In these embodiments, it is clear that the permission to be presented by the user when attempting to gain access to a particular URL is the permission that contains the URL. In other embodiments, any permissions containing a URL that is within the domain of the URL approached by the user may be identified and presented. However, in some cases, requiring that the URL constitute part of the permission, or even requiring that the permission contain a URL that is within the domain of the URL to which access is desired, may be too limiting because such a permission will only be useful for obtaining access to a service located at the specific URL named or one within its domain. Thus, it may be desirable to configure the label such that it does not include any URL, but instead allows the URL indicating the location of the desired service to be determined from another source.

[0068] However, when the user approaches a particular URL, a determination must still be made as to which permission to present. In cases in which the URL is not part of label (and, thus, not part of the permission), this may be accomplished in a number of different ways. In one solution, upon the user approaching the URL, the server hosting the URL may make a request that the user upload a particular permission. Yet another solution involves use of MIME types as described in more detail in Maywah, A.J., "An Implementation of a Secure Web Client Using SPKI/SDSI Certificates", Massachusetts Institute of Technology, pp. 64-68, May 2000, which is hereby incorporated by reference.

[0069] In still another solution, the URL to which the user seeks access may include a piece of information that constitutes an invitation to the user to supply a particular permission, which is done automatically upon the user attempting to access the URL. This approach avoids the step of requiring the user to upload the permission required. Given that the user may not even know the invitation in the URL exists, in some embodiments, the user may be warned in advance of the invitation. This will enable the user to make an informed decision in advance as to whether to proceed to attempt to gain access to the service at the URL.



[0070] In still other solutions, the invitation to supply a particular permission may be included within a web page associated with the URL to which the user seeks to gain access. For example, the invitation may be included within an HTML tag of the web page. The invitation may take several forms. For example, in the preferred embodiment, the invitation is a specific field within the HTML tag. Thus, when the user retrieves the web page associated with the URL, the tag that includes the invitation is retrieved along with the web page. This tag will allow the required credential information to be provided.

[0071] With reference to Figure 5 through Figure 10, several methods of providing secure access to a service on a web server in accordance with preferred embodiments of the present invention are illustrated. With reference to Figure 5, in step 502, a first user is provided access to a label service on a permission web server. In step 504, the first user is allowed to determine, using the label service, a label related to the service. In step 506, a first permission link is created at the permission web server. The first permission link includes the label and a digital signature of the permission web server. The first permission link is provided to the first user in step 508. In step 510, a permission, including the first permission link and a second permission link, is received at the service web server from a second user. The second permission link is created by the first user and includes a digital signature of the first user. In step 512, the digital signatures in the permission are verified. In step 514, it is determined whether an analysis of the permission produces a positive result. If not, in step 516 the process ends. If the analysis produces a positive result, in step 518, the second user is provided access to the service.

[0072] With reference to Figure 6, in step 602, a first user is provided access to a label service on a label server. In step 604, the first user is allowed to determine, using the label service, a label related to the service. In step 606, the label is provided to the user. In step 608, a permission is received at the service web server from a second user. The permission is created by the first user and includes a digital signature of the first user and the label. In step 610, the digital signature in the permission is verified. In step 612, it is determined whether an analysis of the permission produces a positive result. If not, in step 614, the method ends. If the analysis produces a positive result, in step 616, the second user is provided access to the service. In a preferred embodiment, in step 618, it is verified that the first user had the authority to delegate access to the service.

[0073] With reference to Figure 7, in step 702, a first user is provided access to a label service on a permission web server. In step 704, the first user is allowed to determine, using the label service, a label related to the service. In step 706, a first permission link is created at the permission web server. The first permission link includes the label and a digital signature of the permission web server. In step 708, the first user is provided the first permission link. In step 710, a subsequent permission is received at the service web server from a subsequent user. The subsequent permission includes the first permission link, a second permission link (which includes a digital signature of the first user), and at least one intervening permission link (which includes a digital signature of at least one intervening user). In step 712, the digital signature of the permission web server, the first user, and each intervening user in the subsequent permission is verified. In step 714, it is determined whether an analysis of the subsequent permission produces a positive result. If not, in step 716, the process ends. If so, in step 718, the subsequent user is provided access to the service.

[0074] With reference to Figure 8, in step 802, a first user is provided access to a label service on a web server. In step 804, the first user is allowed to determine, using the label service, a label relating to the service on the web server. In step 806, the label is provided to the first user. In step 808, the first user transmits the label to a second user via a messaging system, and in step 810, information based on a public key of the second user and the label is automatically stored on the web server. In step 812, the second user is authenticated with respect to his public key. In step 814, it is determined whether the authentication process produces a positive result. If not, in step 816, the process ends. If so, in step 818, the second user is provided access to the service.

[0075] With reference to Figure 9, in step 902, a first permission is maintained at a permission web server. The first permission includes a label relating to the service and a digital signature of a first user. In step 904, a second user is provided access to the first permission upon the second user authenticating to the permission web server. In step 906, the second user is provided a permission. The permission includes the first permission and a permission link (including the label and a digital signature of the permission web server). In some embodiments, in step 907 the second user delegates the permission to a subsequent user. In step 908, a request to access the service is received at the web server from the second (or subsequent ) user. In step 910, the permission (or subsequent permission) is received at the service web server from the second (or subsequent) user. In step 912, the digital signatures in the permission (or subsequent permission)

are verified. In step 914, it is determined if the verification produces a positive result. If not, the process ends in step 916. If so, in step 918, the second (or subsequent) use is provided access to the service.

[0076] With reference to Figure 10, in step 1002, automatic creation of a first electronic message directed to a plurality of recipients by a first user is facilitated. The first electronic message includes a permission to access the service based on a public key of each recipient and is signed with a digital signature of the first user. In step 1004, a plurality of electronic messages (each including a copy of the first electronic message) is automatically created from the first electronic message. In step 1006, one of the plurality of electronic messages is distributed to each of the plurality of recipients. In step 1008, one of the plurality of electronic messages is received from at least one of the plurality of recipients. In step 1010, the digital signature of the first user in the received electronic message is automatically verified by the web server. In step 1012, it is determined whether the verification process produces a positive result. If not, in step 1014, the process ends. If so, in step 1016, access to the service is provided.

[0077] The foregoing description of the preferred embodiments is provided to enable those skilled in the art to make and use the present invention. The various modifications to these embodiments will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other embodiments without the use of the inventive faculty. Thus, the present invention is not intended to be limited to the embodiments shown herein but is to be accorded the widest scope consistent with the principles and novel features disclosed herein.